



Testimony of:

**Sophia Oberton, MBA**  
*Special Project Coordinator*

Representing the:

**Town of Delmar, Delaware and Maryland  
Delaware Rural Water Association  
Maryland Rural Water Association  
National Rural Water Association**

Before the:

**U.S. Senate Committee on Environment and Public Works  
July 21, 2021**

**Subject:** *Cybersecurity of water infrastructure of small and rural local governmental authorities.*

Good morning, Chairman Carper, Senator Cardin and members of the Committee. I am Sophia Oberton, the Special Project Coordinator with the Town of Delmar in Delaware and Maryland. We have a population of approximately 4,500 persons. My title means I am the lead drinking water operator for the town. I hold a class 4 drinking water operators' license in both Delaware and Maryland. In addition to managing the town's public drinking water supply, I am also the town's Safety Coordinator.

I am honored to testify here today on behalf of all small and rural communities in the United States through my affiliations with the Delaware, Maryland and National Rural Water Associations. I am joined by my mother, Ms. Linda Anderson, and Delmar's Town Manager, Ms. Sara Bynum-King.

Before getting into the substance of my comments, I want to personally thank you, Senator Carper, for being such a good friend and supporter of rural Delaware and rural USA. The rural and small town provisions in your recent legislation, "The Drinking Water and Wastewater Infrastructure Act of 2021," are very much appreciated and you made us so proud when you chose to announce the legislation at the Delaware Rural Water Association headquarters in Milford in April.

The Town of Delmar would like to sincerely thank Congress for the funding we received under the \$1.9 trillion COVID-19 Stimulus Package otherwise known as the American Rescue Plan Act (ARPA).

We received \$930,000 from Delaware and \$2.8 million from Maryland. A significant portion of this funding will be earmarked for water and sewer projects by our local government - we are very appreciative of the assistance.

My three main messages here today regarding cybersecurity protection of small, rural and tribal communities' public drinking water infrastructure are:

First, small communities only operate to serve the public's interests. We are owned and governed by our local citizens through their elected local governments. We only exist to serve the public and are eager to take all feasible and necessary actions to protect the cybersecurity of our public drinking water supplies. This means that any federal initiative to protect the country's public water supplies should be assistance-based. We need help in the form of technical assistance on how to best implement the newest and most advanced cyber protection actions for our specific water infrasource as opposed to a regulatory construct. Additional federal regulation of cybersecurity in water supplies is not the appropriate policy because local governments are eager to adopt the best cyber policies. Again, we need help, not enforcement.

Second, the country's public drinking water supplies are different from other critical infrastructure sectors because we are local governments and nonprofits and because of the very large number of public water supplies; there are 49,775 Community Water Systems (CWSs) in the U.S. and 146,839 Public Water Systems (PWSs).<sup>1</sup>

And third, most U.S. Community Water Systems are small like my town of Delmar. 91percent (45,350) of the country's 49,777 Community Water Systems serve populations of less than 10,000 persons; 89 percent (40,332) serve populations of less than 3,300 persons. That means approximately 90 percent of the country's public water supplies are smaller than my town and I am about to explain the rudimentary nature of Delmar's water cybersecurity system. The water cybersecurity systems of cities like Baltimore and Philadelphia are completely different from the systems of small communities like Delmar that are typical of over 90 percent of the U.S. water public water supplies. Large cities have very complex cybersecurity and SCADA systems to operate and protect their utilities. Because of their complexity, they also have many more potential targets for hostile actors and cyberattacks. On the other hand, their size and economies of scale provide them far greater financial and technical resources to protect their complex systems - and they are doing a very good job of protecting their water supplies. However, any successful cyberattack on a small community that results in drinking water contamination would result in causing psychological panic on a national scale as communities fear their own drinking water supply could be threatened. This is why small communities believe that protecting our water supplies from any cyberattack is just as important as protecting large communities. Large and small communities have a shared mission to protect and enhance the health and safety of our citizens.

We believe that any federal government policy for water cybersecurity must treat small and large communities very differently while recognizing the fundamental differences in the complexity of the water systems, financial resources, and technical capability. For a town the size of Delmar, a \$1,000 dollar cost is a significant expenditure. We only have three licensed drinking water operators who need to implement all safety measures, manage all treatment of the water, read the meters, be on call at night for line breaks, manage the wells, the pumps, and our two water towers, take all the required U.S. Environmental Protection Agency (EPA) tests including the lead tests, operate the chlorine disinfection and pH adjustment processes which require constant monitoring, submit all the test results to the state, exercise our pumps and valves, sample the water for a variety of water quality parameters every day, complete and mail the federally mandated public water quality report every year, respond to any problems that can occur at any time, and keep the water safe and flowing to every citizens' tap every second of every day - including during the pandemic of the last year and half.

---

<sup>1</sup> U.S. EPA, Attachment 1.

In Delmar, we don't have a SCADA (supervisory control and data acquisition) control system or any interface with the internet regarding our water infrastructure assets and fixtures. On the other hand, we do have automated well-pumps, disinfection injection, sodium carbonate mixing technology and pressure monitoring systems. We have to be at the water treatment facility, however, to directly adjust the technological systems to maintain our water safety parameters. Suppose one of the water treatment technologies is not functioning properly. In that case, we receive an alarm message on our cell phone and we must get to the appropriate part of the treatment facility to fix the situation. These urgent messages are a common occurrence. We do have personal computers (PCs) in the office connected to the internet. However, these PCs do not interface with any of the water treatment technologies or our customers' records. We take precautions to protect any data and information on these PCs from potential cyberattacks.

Our wastewater utility does have a rudimentary SCADA system to adjust our secondary wastewater treatment process and ultraviolet light disinfection. Still, that SCADA system is not connected in any manner to the internet, and the operator must be at the wastewater treatment facility to use that SCADA system.

We want the Committee to know that when towns like Delmar need help in operating our water utilities, understanding new and complex federal Clean Water Act (CWA) and Safe Drinking Water Act (SDWA) requirements, receiving the required training to maintain our licenses, and learning about the latest cybersecurity practices, we call our rural water association and ask for assistance from their circuit rider technical assistance providers. These circuit riders will travel directly to our town and focus on our particular issue with our specific water utilities. They have been essential to almost every small and rural community in Delaware, Maryland, and the other states. Circuit riders are funded by Congress each year through the appropriations process - and I would like to express deep gratitude on behalf of every rural and small community for this Committee's support of the funding for our circuit riders every year.

Just this past April, a circuit rider from Delaware Rural Water and another from Maryland Rural Water came to Delmar and spent an entire day helping us complete the very complicated EPA mandated Risk and Resiliency Assessment (RRA) that was authorized in the 2018 America's Water Infrastructure Act (AWIA). I can't imagine how many days this approximately 50-page assessment would have taken us to complete without the direct technical assistance of the rural water circuit riders. We may have been forced to pay a consulting engineer to complete the assessment for us, which would likely cost over \$10,000 - a massive unplanned expenditure for a town our size. This assessment included a review of our cybersecurity plans and every other possible threat (cyber, natural, terrorism, disgruntled personnel, etc.) to our water infrastructure. We certified the completion of the assessment to EPA on April 22nd (the deadline was June 30, 2021).

This exercise did reveal some vulnerabilities to the community, which I will explain shortly. However, it was not the mandated assessment that allowed us to focus on the greatest threats to the public water supply in Delmar - it was the time and experience of the circuit riders that educated us on possible vulnerabilities. It is relevant to note that cybersecurity is a very low to non-existent risk to our town. What the circuit rider did help us realize was that our simple hard-water infrastructure assets were likely our greatest vulnerability. Items like fencing and secure locks on any access to our storage towers, well-houses, pump-houses, and the water treatment technologies in the water treatment facilities' buildings are what we need to monitor and enhance constantly. We do have security and protection for all these assets, but they are likely our most significant vulnerabilities. Also, the circuit riders' assessment allowed us to observe that physical disruption of our drinking water supply is what we need to be most vigilant in preventing and planning for all contingencies. We rely on a series of pumps to keep the distribution system pressurized, the wells pumping, the storage tanks full, the town supplied with drinking water. Any physical harm to this system could leave the town without water, and we assessed this to be our significant threat as opposed to a cyberattack. Our nearest neighboring water supply is the City of Salisbury, Maryland, which is likely too far away to establish

any emergency inter-connection. Therefore, we are planning on all types of contingencies should any worst-case scenario occur.

Again, cybersecurity is not high on the list of potential threats to our community due to our size, limited use of the SCADA systems, and lack of connectivity to the internet. Our greatest threat identified within the parameters of the EPA RRA assessment is likely the physical disruption of the water supply. However, our most significant issue, from our perspective, is the lack of personnel to operate and maintain the public water supply, fulfill the mandatory compliance testing and reporting, and respond to the typical small-scale emergencies in a water distribution system such as line breaks and leaks. We also need to replace our old and failing terracotta sewer lines which are causing a severe inflow and infiltration (I&I) problem for the wastewater utility. The reality is that small towns have limited financial resources, which must be targeted to meet our greatest needs. We would not want to see any new federal cybersecurity initiative or regulation result in the reprioritization of these limited resources to compliance with a new federal cyber program. And we simply can't just increase water rates to cover the cost of new federal requirements. Increasing water rates on our low-income residents can have the unintended consequence of forcing them to go without something they desperately need like food, housing, medical needs, etc.

### **Our Current Water Rates and Financing Information:**

- **Drinking Water (based on meter readings):** Water usage per 1,000 gallons: \$4.00 for residential units and \$5.00 for commercial units. In addition, there is an availability charge flat rate (based on Equivalent Dwelling Units): \$17.45 for residential units and \$17.45 for commercial units.
- **Sewer (based on meter readings):** Per 1,000 gallons: \$5.50 for residential units and \$7.00 for commercial units. In addition, there is a sewer front footage charge (based on Equivalent Dwelling Units): \$35.00 for residential units and \$35.00 for commercial units.
- **Current Debt to Federal Funding Program** (U.S. Department of Agriculture, Drinking Water State Revolving Fund or Clean Water State Revolving Fund): \$3,316,740.00

### **Two Essential Issues in Advancing Any New Cybersecurity Initiative in Rural and Small Communities:**

Small, rural and tribal communities support the model that Congress adopted in crafting the Risk and Resiliency requirement in AWIA 2018 that (1) limited the federal government's authority to review the content of RRAs and (2) only required that communities "certify" completion of the RRA and not submit the content of the RRAs for review or federal cataloguing.

Any potential new federal cybersecurity program for U.S. public water supplies should use this model as the starting point and make additional improvements by adopting two essential principles or characteristics.

One, any cybersecurity program should be very "scalable," meaning it must recognize that the complexity of water cybersecurity systems in a small community like Delmar is not remotely similar to a large community. Again, Delmar, with a population of 4,500 people, does not have a SCADA system or internet access for our drinking water systems. As we are larger than over 90 percent of the approximately 50,000 U.S. Community Water Systems, this situation is typical among many small communities. Like those of my colleague testifying with me today, large metropolitan drinking water utilities are immensely more complex and their communities have vastly more resources to take the necessary protective actions for their SCADA and cybersecurity systems. And as my colleague testifies, they are responsibly taking those precautions without any current federal mandate because that is their purpose - to provide for the public welfare.

Second, any new federal initiative should also provide new technical assistance to help small communities with implementation. For the smallest communities, the burden of performance should be far less than the RRA program. Again, the scalability of the degree of commitment is essential to limit the federal program from resulting in the unintended consequence of wasting precious and limited local public funds. Over 54 percent of the approximately 50,000 U.S. Community Water Systems serve populations of less than 500 persons.<sup>2</sup> Many will not have full-time operators, will definitely need technical assistance to manage any new program, are fundamentally different in their complexity compared to a large city, and cybersecurity enhancement will very rarely be their priority for protecting their public.

The most successful approach for making progress in environmental compliance for small and rural Community Water Systems and overcoming their lack of technical resources has been the circuit rider concept, created by Congress, which provides all small communities with the shared technical resource of an expert with experience in water utility operations and compliance. This expert can travel directly to small, rural and tribal communities, as needed, to assist with rule compliance and generally eliminate the need for civil-enforcement. Additionally, the circuit riders only act in the community's interest which allows them to identify the most economical solution and provide the best advice for local decision-makers. What small and rural communities want and need is to know how to comply simply and affordably – and similarly, how to operate and maintain their water utilities. Consistent with our request that any new federal cybersecurity regulation not circumvent local priorities and result in unnecessary costs to limited public funds, we are likewise concerned that any new mandate could distract the existing circuit riders' time and resources away from what small communities in Delaware, Maryland and the rest of states see as their most pressing concerns. We urge you to be mindful of this dynamic when considering any new federal policies for cybersecurity plans in the water sector.

The National Rural Water Association (NRWA) has urged Congress to adopt a plan that relies on these two essential principles or characteristics in any federal cybersecurity initiative.<sup>3</sup> Additionally, by collaborating the water sector, and utilizing the existing state rural water associations' network that water supplies rely on for security initiatives and education, the federal government could (1) rapidly assess all of the water supplies efficacy in protecting their cyberinfrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all water supplies. Upon adoption/completion of a cybersecurity proposal, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state, and local authorities could easily track which communities have taken the initiative to secure their cyberinfrastructure. The contents of each plan could be combined with each community's RRA and Emergency Response Plans. Such an approach would promote local support for security initiatives essential to ensure security protection because only local experts can identify the most vulnerable elements in the community and detect immediate threats.

In closing, Mr. Chairman, I want to thank you again on behalf of all small and rural communities for your continued help and assistance. Moreover, I want to thank all the Senators on the Committee for your consideration of our issues. This Committee is very important to rural and small town America; every federal dollar that has been granted to the many thousands of small towns to build, expand, and maintain their drinking water and wastewater infrastructure through the state revolving funds was authorized by this Committee. Also, this Committee likewise authorized every federal regulation under the Safe Drinking Water or the Clean Water Act.

We are grateful to testify today and thankful for the numerous opportunities this Committee has provided rural America to testify and be included in the crafting of water and environmental legislation.

---

<sup>2</sup> U.S. EPA, Attachment 1.

<sup>3</sup> NRWA, May 12, 2021, Attachment 2.

## Attachment 1.

### U.S. EPA, Government Performance and Results Act Data (June 2021)

#### GPRA Inventory Summary Report

Population Size Category	<=500		501-3,300		3,301-10,000		10,001-100,000		>100,000		# of Systems	Population Served Count
	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count	# of Systems	Population Served Count		
PWS Type Code												
CWS	26,977	4,548,387	13,355	19,229,892	5,018	29,511,268	3,960	114,113,454	445	147,693,996	49,755	315,096,997
NTNCWS	15,030	2,074,858	2,466	2,637,868	164	908,392	38	812,466	1	203,375	17,699	6,636,959
TNCWS	76,326	7,092,346	2,972	2,786,182	75	387,952	12	247,616			79,385	10,514,096
<b>Grand Total</b>	<b>118,333</b>	<b>13,715,591</b>	<b>18,793</b>	<b>24,653,942</b>	<b>5,257</b>	<b>30,807,612</b>	<b>4,010</b>	<b>115,173,536</b>	<b>446</b>	<b>147,897,371</b>	<b>146,839</b>	<b>332,248,052</b>

SUBMISSIONYEARQUARTER is equal to 2021Q1  
and NPM\_CANDIDATE is equal to / is in Y



May 12, 2021

The Honorable Gary Peters  
Chairman  
Committee on Homeland Security &  
Governmental Affairs  
U.S. Senate  
Washington, DC 20510

The Honorable Rob Portman  
Ranking Senator  
Committee on Homeland Security &  
Governmental Affairs  
U.S. Senate  
Washington, DC 20510

The Honorable Bennie Thompson  
Chairman  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

The Honorable John Katko  
Ranking Member  
Committee on Homeland Security  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Peters, Ranking Senator Portman, Chairman Thompson and  
Ranking Member Katko:

The National Rural Water Association's (NRWA) over 30,000 small and rural community members with drinking water and/or wastewater supplies are very eager to initiate a partnership with the U.S. Department of Homeland Security (DHS) to secure small and rural community water utilities from cyber-attacks. The U.S. has approximately 50,000 community water supplies and 16,000 wastewater supplies - typically under various forms of local governments.

Approximately 90 percent of these water utilities are small, serving fewer than 10,000 persons. As the two most recent water cyber-attacks in Florida and Kansas have indicated, small communities can be a target of cyber-criminals including international actors. By implementing a few relatively simple actions, these water utilities could greatly decrease their vulnerability to future cyber-attacks. With a small additional cost for system infrastructure, many water utilities can take immediate essential actions such as removing insecure remote access (SCADA protection), performing a risk assessment, raising awareness of the issue, applying firewalls, providing multi-factor authentication, securing user accounts, limiting access to accounts, inventorying mobile access devices, and implementing protective policies for former employees.

*The National Rural Water Association is the country's largest public water utility organization with over 30,000 members. Safe drinking water and wastewater service are generally recognized as the most essential public health, public welfare, and civic necessities.*

By collaborating with small and rural communities and utilizing the existing network that water supplies rely on for security initiatives and education, the department could (1) rapidly assess all small water utilities efficacy in protecting their cyberinfrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all small water supplies. Upon adoption/completion of a cybersecurity plan, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state, and local authorities could easily track which communities have taken the initiative to secure their cyberinfrastructure. The contents of each plan could be combined with each community's vulnerability assessment and emergency response plan.

In the past, similar types of security initiatives have been uniquely successful because they expeditiously advanced measurable security initiatives in water systems with the support of the local communities. For compliance with the Bioterrorism Act of 2002, for example, over 90 percent of small community water supplies relied on the rural water cooperative approach for completing security vulnerability assessments (VA) in a matter of months – at no cost to the communities. The 2018 America's Water Infrastructure Act (AWIA) requires updating these assessments by June 30, 2021. However, no federal funding has been provided to assist with compliance. The compliance rate for the revised assessments should be dramatically higher due to the existing network and outreach. The AWIA requirement for communities to adopt revised VAs was appropriately crafted by Congress in such a way to allow each community to address and prioritize their own vulnerabilities. This type of local tailoring is essential to crafting the most protective security plans because every community has a unique set of vulnerabilities. It also has the additional benefit of promoting local support for security initiatives versus a uniform regulatory approach, which is often costly and results in local resistance because it forces communities to dedicate limited funding and resources to something they see as unnecessary.

We urge you to initiate a similar approach with the Department of Homeland Security to rapidly evaluate and improve the cybersecurity measure in all small water utilities. We have recently partnered with the Mission Critical Global Alliance (MCGA) to develop the necessary protocols for a comprehensive continuous cyber assessment and education program and we would be eager for DHS collaboration on the content of the protocols and support to implement the protocols. With DHS support, we believe we could assess, measure, and improve every small and rural community's water infrastructure in a matter of months.

Small and rural water utilities want to take all necessary precautions to protect their utilities and the public. What is needed is to know how to take the most appropriate actions and make them simple and cost-effective. Local support and responsibility are essential to ensuring security protection because only local experts

*The National Rural Water Association is the country's largest public water utility organization with over 30,000 members. Safe drinking water and wastewater service are generally recognized as the most essential public health, public welfare, and civic necessities.*

can identify the most vulnerable elements in the community and detect immediate threats. A national collaborative cybersecurity water supply protection initiative should result in communities focusing enthusiastically on enhancing local security based on local risks. The best cybersecurity protection of a water utility is an educated and responsible local governing structure and operator.

Again, we are eager to partner with DHS in assessing the needs of every small water utility. Together, we can provide the appropriate education and technical assistance to ensure all necessary protective actions are conducted in a timely manner. We can also provide the federal government and Congress with the documented baseline assessment of the cybersecurity statutes and corresponding corrective actions in all small water utilities in the U.S.

Thank you for your consideration,

Sincerely,



Matthew Holmes, CEO

CC: Senators Warner and Rubio, Select Committee on Intelligence  
Senator King and Representative Gallagher, CyberSpace Solarium Commission  
Anne Neuberger, Deputy National Security Advisor for Cyber & Emerging  
Technologies  
Brandon Wales, Acting Director of the Cybersecurity and Infrastructure Security  
Agency

Image 1



Image 2



Image 3



Image 4



Image 5



Image 6



Image 7



Image 8



Image 9



Image 10



Image 11



Image 12



Image 13



Image 14



Image 15



Image 16



Image 17



Image 18



Image 19



Image 20



Image 21



Image 22



Image 23



Image 24

